07-24-00

Case Docket No. PHO 99,534

THE COMMISSIONER OF PATENTS AND TRADEMARKS, Washington, D.C. 20231

Enclosed for filing is the patent application of Inventor(s):
ANDREAS MUHLBERGER, STEFAN POSCH

For: DATA CARRIER FOR THE STORAGE OF DATA AND CIRCUIT ARRANGEMENT
FOR SUCH A DATA CARRIER

ENCLOSED ARE:
[X] Associate Power of Attorney;
[X] Information Disclosure Statement, Form PTO-1449 and copies of
     documents listed therein;
[ ] Preliminary Amendment;
[X] Specification (29 Pages of Specification, Claims, & Abstract);
[X] Declaration and Power of Attorney:
     (1 Page of a [ ]fully executed [X]unsigned Declaration);
[X] Drawing (2 sheets of [ ]informal [X]formal sheets);
[X] Certified copy of a EUROPEAN application Serial No.99890248.0;
[ ] Other: ;
[ ] Assignment to   .

FEE COMPUTATION

CLAIMS AS FILED				
FOR	NUMBER FILED	NUMBER EXTRA	RATE	BASIC FEE - 690.00
Total Claims	15 - 20 =	0	X $18 =	0.00
Independent Claims	3 - 3 =	0	X $78 =	0.00
Multiple Dependent Claims, if any			$260 =	0.00
TOTAL FILING FEE			=	$690.00

**Please charge Deposit Account No. 14-1270 in the amount of
the total filing fee indicated above, plus any deficiencies. The
Commissioner is also hereby authorized to charge any other fees
which may be required, except the issue fee, or credit any
overpayment to Account No. 14-1270.**

[ ]Amend the specification by inserting before the first line the
sentence: --This is a continuation-in-part of application Serial
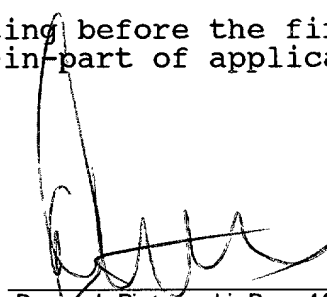No.   , filed   .--.

Daniel J. Piotrowski, Reg. 42,079
Attorney
(914) 333-9633
U.S. Philips Corporation
580 White Plains Road
Tarrytown, New York 10591
F:\WPDOCS\PW\MW14PWAO.MAO.doc

Data carrier for the storage of data and circuit arrangement for such a data carrier.

The invention relates to a data carrier as defined in the opening part of Claim 1.

The invention further relates to an electrical circuit arrangement as defined in the opening part of Claim 1.

5   The invention further relates to a method as defined in the opening part of Claim 13.

Such a data carrier, such a circuit arrangement and such a method are known

10   from the document WO 97/29454. The known data carrier takes the form of a so-called smart card.

The known data carrier has a contactless first interface for the contactless communication with a communication device. During contactless communication a transmission of energy to the data carrier for the purpose of generating a supply voltage for

15   the circuit arrangement of the data carrier as well as an exchange of data between the data carrier and the communication device are realized by means of an inductive coupling between a transmission coil of the communication device and a transmission coil of the contactless interface with the aid of a high-frequency carrier signal.

The known data carrier further has a contact-bound second interface for the

20   contact-bound communication with a communication device. The contact-bound interface is constructed in accordance with the ISO 7816 standard, thus enabling a supply voltage for the circuit arrangement to be applied and data to be exchanged via the contacts of this interface.

The known data carrier has memory means for the storage of data in a plurality of storage locations, the memory means taking the form of a solid-state memory of

25   the EEPROM type.

A first memory access means can access a first storage location, the first memory access means being formed by a first operating system which has become known under the trademark "Mifare". This first operating system supports a first communication protocol, which guarantees an authenticated access by the first operating system in

accordance with the ISO/IEC DIS 9798-2 standard during communication via the contactless interface and during access to the first storage location. An essential feature of this authentication is the secrecy of keys stored in the first storage location.

The second storage location can be accessed by a second operating system,
5   namely a user operating system, via a second memory access means, the second memory access means being formed by parts of the first operating system. The second operating system can support an arbitrary second communication protocol.

The known data carrier further includes access enabling means which ensure that during communication via the contactless interface the first storage location can be
10   accessed only by the first operating system and that during communication via the contact-bound interface the second storage location can be accessed only by the second operating system. The access enabling means are realized by an access enabling stage during cooperation with the respective memory access means by which access is effected. The access enabling stage is stored unalterably in a ROM and enables or inhibits the access to the
15   various storage locations by the memory access means via access authorizations stored in it.

Thus, in the know data carrier the first communication protocol provides a variable first protection and the access enabling means provide an unalterable second protection, i.e. together they provide double protection against unauthorized access to the data in the first storage location.

20   In practice, the known data carrier is often used at two different system operators. The first system operator may be, for example, a transport company which in the case of communication via the contactless interface should access data stored in the first storage location and representing, for example, transportation units, by means of the first operating system. The second system operator may be a banking company which in the case
25   of communication via the contactless interface should access data stored in the second storage location and representing, for example, amounts of money, with the aid of the second operating system, which is generally implemented independently of the first operating system because of complex requirements imposed by the banking enterprise. It is therefore evident that in the case of such a configuration both system operators require a maximal protection of
30   the data stored in the respective storage locations against unauthorized access by the operating system of the other system operator both from their own point of view and from their customers' point of view and that the access allocation means fully meet this requirement.

However, in the case of cooperation of the system operator it may be desirable that the banking company mentioned in the above example should access the data of the transport company as stored in the first storage location on the data carrier (for example data about transportation units) for the direct settlement of services of the transport company. In actual practice this may mean that in a communication device (bank terminal) of the banking company it should be possible to enter data representative of transportation units in the storage location of the transport company, i.e. in the first storage location.

With the known data carrier there would be a first possibility of allowing cooperation between the system operators in that during a communication via the contact-bound interface the second operating system is given the right, by means of an extension of the first communication protocol, to access the first storage location via the first operating system in accordance with the first communication protocol if the keys necessary for the authorization are known.

However, this possibility is not used. This is because it would require knowledge of the keys stored in the first storage location, i.e. in the storage location of the transport company, by the communication device used by the banking company for the communication with the data carrier. Thus, it would allow authentication but at the same time it would violate the essential feature of the authentication, namely the secrecy of the keys. This would undermine the first protection in a highly undesirable way.

With the known data carrier there would also be a second possibility of cooperation between the system operators, in which case the authentication by means of the keys in accordance with the first communication protocol is omitted. However, the first protection demanded by the transport company, to preclude unauthorized access to the data in the first storage location, would then be eliminated completely.

It is an object of the invention to preclude the problems associated with a data carrier of the type defined in the opening part of Claim 1, with an electrical circuit arrangement of the type defined in the opening part of Claim 7, and with a method of the type defined in the opening part of Claim 13 and to provide an improved data carrier, an improved circuit arrangement and an improved method so as to enable a cooperation of two system operators with an unchanged high degree of protection against unauthorized access to the data stored in the first storage location.

According to the invention, in order to achieve said object with a data carrier of the type defined in the opening part of Claim 1, the characteristic features defined in the characterizing part of Claim 1 have been provided.

According to the invention, in order to achieve said object with a circuit

5   arrangement of the type defined in the opening part of Claim 7, the characteristic features defined in the characterizing part of Claim 7 have been provided.

According to the invention, in order to achieve said object with a method of the type defined in the opening part of Claim 13, the characteristic features defined in the characterizing part of Claim 13 have been provided.

10   By providing the characteristic features in accordance with the invention as defined in Claims 1, 7 and 13 it is achieved in a highly advantageous manner that after verification of an access authorization and receipt of a positive result of the verification of the access authorization the second memory access means can access the first storage location via additional memory access means not included in the second memory access means and

15   via the first memory access means.

The provision of the additional memory access means in the data carrier and in the circuit arrangement has the advantage that a cooperation of two system operators can be made possible in a simple manner while a high degree of security with regard to unauthorized access to storage locations of the two system operators remains guaranteed for both system

20   operators.

A second advantage is obtained in that the inhibition of a direct access to the first storage location by the second memory access means achieved by means of the access enabling means is maintained and at the same time an access to the first storage location by the second memory access means via the first memory access means is possible after a

25   verification of access authorizations for the protection against unauthorized access to the first storage location.

A third advantage is obtained in that a fully consistent access is assured as a result of the access of the second memory access means to the data in the first storage location with the aid of the first memory access means. This ensures an accessibility of said

30   data during a communication based on a communication protocol of the first memory access means.

A fourth advantage is that an individual configuration of the access authorizations as well as a flexible management of these access authorizations are guaranteed during the life of a data carrier in accordance with the invention, because a system operator,

for example a transport company, can assign, refuse and modify access authorizations without any problems during a communication between the data carrier and the contactless communication device.

5   The provision of the characteristic features of the invention as defined in Claims 2 and 8 yields the advantage that it is possible to use software routines which are already available in the first memory access means, enabling the characteristic features in accordance with the invention to be realized in a particularly simple manner.

The provision of the characteristic features of the invention as defined in Claims 3, 9 and 14 yields the following advantages. First of all, the advantage is obtained that

10   during a verification of an access code with the aid of the access code verification means an access code is used which can be computed from the data of the first storage location. This has proved to be particularly advantageous in view of secrecy of the keys stored in the first storage location, because it is not a key itself that used for the verification but an access code which can be calculated from said key. Secondly, the use of an access code which can be

15   applied by the second memory access means during the verification of the access authorization is highly advantageous because this provides a maximal flexibility as regards the source of this access code capable of being applied. Thus, an applicable access code may be stored in the data of the second storage location or may be calculated from said data. In this respect it has proved to be particularly advantageous when an applicable access code is

20   communicated in an encrypted manner during communication between the data carrier and a communication device via one of the two interfaces.

In a data carrier in accordance with the invention and a circuit arrangement in accordance with the invention the provision of the characteristic features of the invention as defined in Claim 4 and Claim 10 has proved to be highly advantageous in two respects. First

25   of all, the execution of the calculation is speeded up by the provision of dedicated access code calculation means for the calculation of a calculable access code, as a result of which a considerably shorter duration of the communication between the data carrier and a communication device is possible. Secondly, the execution of a triple DES encryption process in accordance with the ISO/IEC 10116 standard prevents a key on which the

30   calculable access code is based can be calculated from an access code derived from this key by the use of an inverse encryption process.

In addition, the provision of the characteristic features of the invention as defined in Claims 5, 11 and 15 has proved to be highly advantageous. This is because it is thus achieved that for the protection against unauthorized access to the first storage location,

in addition to the verification of the access code during the verification of access
authorizations, a check on access conditions (writing, reading) is performed. This ensures in a
simple manner that even in the case of correspondence of an applicable access code to a
calculable access code an additional check is carried out before finally a positive result of the
5   verification of the access authorization is obtained upon an additional correspondence of said
access conditions. As a result of this measure, a hierarchical structure of the allocation of the
access authorization can be provided, thus enabling a maximal protection against
unauthorized access to the first storage location to be achieved in a simple manner.

For a data carrier in accordance with the invention and a circuit arrangement in
10   accordance with the invention the provision of the characteristic features of the invention as
defined in Claims 6 and 12 has proved to be advantageous because this guarantees a
production at minimal costs in the case of production in correspondingly high quantities.

The above-mentioned as well as further aspects of the invention will become
apparent from the example of an embodiment described hereinafter and will be elucidated
15   with reference to this example.

The invention will now be described in more detail with reference to the
drawings, which shows an embodiment given by way of example but to which the invention
20   is not limited.

Figure 1 is a block diagram which diagrammatically shows a data carrier
having additional memory-access means.

Figure 2 is a flow chart which shows a method of accessing memory means of
the data carrier shown in Figure 1.

25

Figure 1 is a block diagram which shows a data carrier 1 for the storage of
data, which takes the form of a smart card and which is adapted to communicate with a first
communication device 2 and a second communication device 3. Such a smart card is formed
30   by a plastic card which accommodates a semiconductor chip forming an electrical circuit
arrangement and is known since long.

The first communication device 2 is adapted to provide contactless
communication with the data carrier 1 and includes a first transmit/receive means 4. The first
transmitting/receiving means 4 is adapted to modulate the amplitude of a carrier signal in

accordance with first transmission data SD1, which can be applied to the first
transmitting/receiving means 4 by a first communication means, not shown in Figure 1. The
amplitude-modulated carrier signal is applied to a transmitting/receiving antenna array 5 and
is radiated by this array. Conversely, differences in the load of the radiated amplitude-

5   modulated carrier signal can be detected as a load modulation by the first
transmitting/receiving means 4 and can be applied to the first communication means as first
receiving data ED1 after demodulation. In the present case the transmitting/receiving antenna
array 5 takes the form of a primary coil of a communication coil pair 6 required for the
contactless communication.

10   The second communication device 3 is adapted to provide contact-bound
communication with the data carrier 1 and includes a second transmitting/receiving means 7.
The second transmitting/receiving means 7 includes contact means 8 of a contact pair 9
required for the contact-bound communication, which contact means 8 consist of pin-type
contacts. The contact means 8 comply with the ISO 7816 standard. During contact-bound

15   communication the second transmitting/receiving means 7 can apply second receiving data
ED2 to a second communication means, not shown in Figure 1, and the second
communication means can apply second transmitting data SD2 to the second
transmitting/receiving means 7. The second transmitting/receiving means 7 further has first
level adjustment means, which serve for adjusting signal levels of the second

20   transmitting/receiving data SD2 and the second receiving data ED2.

               The data carrier 2 has a contactless first interface 10 for the communication
with the first communication device 2. The first interface 10 includes a secondary coil 11 of
the communication coil pair 6, which is connected to circuit parts of the first interface,
namely to a first supply voltage means 13 included in an electrical circuit arrangement 12 of

25   the data carrier 1 and to a first signal conversion means 15 included in the electrical circuit
arrangement 12.

               When a carrier signal is received by means of the secondary coil 11 the first
supply voltage means 13 generates a first supply voltage V1 from the received carrier signal,
which first supply voltage serves to provide the electrical power supply of the electrical

30   circuit 12 during contactless communication. When a nominal value of the first supply
voltage V1 appears the first supply voltage means 13 supply a first starting signal POR1 to a
first operating system 16.

               Upon reception of the carrier signal the first clock generator 14 generates a
first system clock signal CLK1. The first system clock signal CLK1 is applied to the first

signal conversion means 15 for the purpose of synchronizing the communication between the first communication device 2 and the first interface 10. Moreover, the first system clock signal CLK1 is applied to the first operating system 16 as an operating clock signal for the purpose of synchronizing the processing of first reception information EI1 and first

5   transmission information SI1, which can be exchanged bidirectionally between the signal conversion means 15 and the first operating system 16.

When the data carrier 1 comes in the proximity of the first communication device 2 and a carrier signal is transmitted via the communication coil pair 6, the data carrier 1 is located within a communication range of the first communication device 2. When the

10   data carrier 1 is within the communication range the first supply voltage V1 for the electrical circuit arrangement 12 is built up upon reception of the carrier signal, which has a frequency of 13.56 MHz in the present example, after which the system clock signal CLK1 is generated and subsequently the processing by the first operating system 16 is started by means of the starting signal POR1. Subsequently, the first operating system 16 effects a selection in

15   accordance with a first communication protocol to select a single data carrier 1 from a plurality of data carriers 1 which may be present within the communication range, after which communication can be established with a selected data carrier 1. Such a selection in conjunction with contactless communication is common practice.

During contactless communication the received carrier signal is applied to a

20   demodulator included in the first signal conversion means 15, which demodulator is adapted to demodulate the amplitude-modulated carrier signal and to supply first reception information EI1 to the first operating system 16. During contactless communication the first operating system 16 applies first transmission information SI1 to a modulator included in the first signal conversion means 15, the modulator being adapted to effect a load modulation of

25   the carrier signal in accordance with the first transmission information SI1.

The data carrier 1 further includes memory means 17 for the storage of data. Such data may represent, for example, amounts of money, transportation units or personal data of a user.

The first operating system 16 is formed by a microprocessor and a first

30   program that can be executed by the microprocessor, as is generally known. The first operating system 16 thus forms a first memory access means 18, arranged between the first interface 10 and the memory means 17, for accessing the memory means 17.

The first memory access means 18 enable access to data stored in the memory means 17 of the electrical circuit arrangement 12. During access to data stored in the memory

means 17 it is possible to write data and to read data. Apart from the access, it is possible to carry out said first communication protocol and arithmetic operations with the aid of a first data processing means 19 included in the first memory access means 18. In accordance with the first communication protocol an authentication during the access to the first storage

5   location 22 has been provided, the arithmetic operations being used for the authentication, as will be described hereinafter.

The data carrier further comprises access enabling means. During access to the memory means 17 by the first memory access means 18 the access enabling means are formed by an access enabling stage 21 together with the first data processing means 19. The

10   access enabling stage 21, which is formed by a ROM, unchangeably stores access authorizations ZE corresponding to all the addressable access addresses ZA of the memory means 17. For example, a logic one as the access authorization ZE(n) corresponding to the access address ZA(n) indicates that access to the access address ZA(n) by the first memory access means 18 is allowed, while a logic zero as the access authorization ZE(m)

15   corresponding to the access address ZA(m) indicates that access to the access address ZA(m) by the first memory access means 18 is not allowed.

A first division of the memory means 17 in the data carrier 1 into a first storage location 22, a second storage location 23 and a third storage location 24 is realized by means of the access enabling means, the access authorizations stored in the access enabling

20   stage 21 only enabling the first storage location 22 to be accessed by the first memory access means 18. The access authorizations ZE also enable the third storage location 24 to be accessed by the first memory access means 18, which storage location can also be accessed by a second memory access means, but this will not be considered any further here.

The data carrier 1 further has a second division of the first storage location 22

25   into sectors. Each sector is made up of four blocks, each block comprising sixteen bytes. Each sector has a sector trailer formed by the fourth block. The sector trailer stores a first key and a second key. The keys serve as a basis for the authentication during access to the first storage location 22.

During the authentication in accordance with the first communication protocol

30   the first communication device 2 generates a first random number, which is preserved in the first communication device 2 during the authentication, and the first data processing means 19 generates a second random number, which is preserved in the first data processing means 19 during the authentication. These two random numbers are transmitted between the data carrier 1 and the first communication device 2 and, on the one hand, the second random

number is encrypted with a third key in the first communication device 2 and, on the other hand, the first random number is encrypted by the first data processing means 19 with the first key of the sector addressed with the access address ZA. The two encrypted random numbers are communicated between the data carrier 1 and the first communication device 2.

5   In the first communication device 2 the encrypted first random number is decrypted by means of the third key, yielding a first decrypted random number. In the first data processing means 19 the encrypted second random number is decrypted by means of the first key, yielding a second decrypted random number. The authentication for access to the data in the sector addressed by means of the access address ZA is completed successfully if in the first

10   communication device 2 the preserved first random number corresponds to the first decrypted random number and if in the first data processing means 19 the preserved second random number corresponds to the second decrypted random number. This implies that the first key and the third key are identical or, phrased differently, that the first communication device 2 must know the key of the sector addressed with the access address ZA.

15   In addition to the two keys, the sector trailer stores a sector access condition with the aid of which the access can be controlled for each sector. This is to be understood to mean that the data of a first sector can be accessed only for data writing, while a second sector is accessible only for data reading. Furthermore, a third sector may enable both reading of data and writing of data. Finally, a fourth sector may inhibit both writing and reading of

20   data, which is used for example in the case of data which is employed exclusively during processing of the first operating system 16 and which should consequently be protected against access during communication.

                   The data carrier 1 further has a contact-bound second interface 25 for the communication with the second communication device 3. The second interface 25 has a

25   contact array 26 of the contact pair 9, whose contact faces can be brought into contact engagement with the contacts of the contact means 8. A first group of connections of the contact array 26 is connected to a circuit part of the second interface 25, i.e. to a second supply voltage means 27 included in the electrical circuit arrangement 12. A second group of connections of the contact array 26 is connected to a further circuit part of the second

30   interface 25, i.e. to a second clock generator 28 included in the electrical circuit arrangement 12. A third group of connections of the contact array 26 is connected to a further circuit part of the second interface 25, i.e. to a second signal conversion means 29 included in the electrical circuit arrangement 12, as provided for in the ISO 7816 standard.

By means of the first group of connections a voltage can be applied to the second supply voltage means 27. The second supply voltage means 27 generates a second supply voltage V2 from said voltage, which second supply voltage serves for electrically powering the electrical circuit arrangement 12 in the case of contact-bound communication.

5   When a nominal value of the second supply voltage V2 occurs the second supply voltage means 27 supply a second starting signal POR2 to a second operating system 30.

The second clock generator 28 can be energized with a clock signal via the second group of connections and, when energized, generates a second system clock signal CLK2. The second system clock signal CLK2 is applied to the second operating system 30 as

10   an operating clock signal for the purpose of synchronizing the processing of second reception information EI2 and second transmission information SI2, which can be exchanged bidirectionally between the second signal conversion means 29 and the second operating system 30.

The second signal conversion means 29 is energized via the third group of

15   connections and effects a level adjustment of the second reception information EI2 and the second transmission information SI2 during communication via the second interface 25.

The second operating system 30 is formed by the microprocessor and a second program which is stored in the ROM and which can be executed by the microprocessor, a second data processing means 31 and an interface means 32 of the second operating system

20   being shown in Figure 1. With the aid of the second data processing means 31 it is possible to carry out a second communication protocol. The second communication protocol provides for an authentication in the case of access to the second storage location, which authentication during access to the second storage location will not be described in any further detail. The second communication protocol further provides for encrypted contact-

25   bound communication, as a result of which the second reception information EI2 supplied by the second signal conversion means 29 is subsequently decrypted by the second data processing means 31 and is then applied to the interface means 32.

The data carrier 1 further has a second memory access means 33 between the second interface 25 and the memory means 17 to access the memory means 17. The second

30   memory access means 33 includes the interface means 32, which comprises an access request buffer 34, a status reception buffer 35 and an access data buffer 36.

In the case of access to the memory means 17 by the second memory access means 33 access parameters ZP are transmitted from the second operating system 30 to the first operating system 16 with the aid of the access request buffer 34 and are processed by the

second memory access means 33. The access parameters ZP to be transmitted are, for example, an access address ZA, a first access code ZC1 and a first access condition ZB1. A first access code ZC1 may be, for example, a password. A first access condition ZB1 may, for example, specify that it has been requested to write data into the memory means 17 or to

5   read data from the memory means 17.

With the aid of the status reception buffer 35 an access status ZS can be transmitted from the first operating system to the second operating system and can thus be transmitted to the second data processing means 31, the access status ZS indicating a successful access to the memory means 17 in a first status or an unsuccessful access in a

10   second status.

When the first status is indicated the data addressed with the access address ZA can be accessed, as will be described in greater detail with reference to a first example of use. When the second status is indicated the access to the memory means 17 by the second operating system 30 should be discontinued.

15   In accordance with the second communication protocol the access status ZS and, if applicable, also the data to be applied to the second data processing means 31 from the access data buffer 36 is subsequently encrypted by the second data processing means 31 and is supplied to the second signal conversion means 29 as second transmission information SI2.

The second memory access means 33 includes an access approval means 37

20   which, together with the access enabling stage 21, forms access enabling means in the case of access to the memory means 17 by the second operating system 33. With the aid of the access approval means 37 the second memory access means 33 can verify an access authorization ZE on the basis of an access address ZA applied via the access request buffer 34. When an access authorization ZE is received the access approval means 37 access the data, defined by

25   the access address ZA, in the second storage location 23 or the third storage location 24 of the memory means 17. During the access data is exchanged either between the second storage location 23 or the third storage location 24 and the access data buffer 36 via the access approval means 37. Furthermore, the access approval means 37 apply the access status ZS to the second data processing means 31 of the second operating system via the status

30   reception buffer 35.

During access of the second memory access means 33 to the memory means 17, the second memory access means 33 is allowed exclusive access the second storage location 23 and access to the third storage location owing to the interrelated storage of the access addresses ZA and access authorizations ZE in the access enabling stage 21.

The operation of the smart card, i.e. of the data carrier 1 in accordance with the invention, will now be explained hereinafter with reference to a first example of use of the data carrier 1 in the embodiment of the invention shown in Figure 1. In this first example of use it is assumed that the data carrier 1 is made available by a first system operator, namely

5   by a banking company as an electronic wallet.

Amounts of money in the form of money data GD can be entered or withdrawn at a bank terminal during an access to the second storage location 23 of the data carrier 1 after identification of a user. Entry or deduction of the amounts of money is effected during a contact-bound communication between a bank terminal, which is equipped with the

10   second communication device 3 for contact-bound communication, and the contact-bound second interface 25 of the data carrier 1. In the first example of use it is assumed that the user of the data carrier wishes to transfer one hundred Euro from his account with the banking company into the electronic wallet, for which purpose money data GD corresponding to the one hundred Euro must be stored in the memory means 17. For this purpose, the user inserts

15   the smart card into a slot of the bank terminal, upon which a contact bound communication is started.

In the course of the subsequently started communication between the second interface 25 and the second transmitting/receiving means 7 of the second communication device 3 second transmission data SD2 to be entered and representing one hundred Euro are

20   communicated to the second signal conversion means 25. The second signal conversion means 25 generates second reception information EI2 from the second transmission information SD2, the content of this second reception information, in accordance with the first example of use, relating to the addition of money data GD corresponding to one hundred Euro to the data of the second storage location 23 of the memory means 17. The content now

25   consists of the access parameters ZP, which comprise an access address ZA, i.e. the access address ZA of the electronic wallet, a first access condition ZB1, i.e. a first access condition ZB1 corresponding to an entry, and the money data GD to be entered and corresponding to the one hundred Euro.

The second reception information EI2 is received by the second data

30   processing means 31 and is decrypted. The access parameters ZP are transferred to the access request buffer 34.

In accordance with the access address ZA the first access approval means 37 of the second memory access means 33 determines whether a read and write access authorization ZE for money data GD addressed with the access address ZA is available for

the applied access address ZA in the second storage location 23 of the memory means 17.

When this access authorization ZE is available the first access approval means 37

subsequently gains access to the old money data GD stored in the second storage location 23

at the access address ZA so as to read the old money data GD. In the first example of use said

5   old money data GD correspond to an amount of twenty Euro. The old money data are

transferred from the first access approval means 37 to the second data processing means 31

via the access data buffer 36, which data processing means adds the money data GD to be

entered to the old money data GD. This results in new money data GD representing one

hundred and twenty schilling, which new money data is transferred from the second data

10   processing means 31 to the first access approval means 37 via the access data buffer 36. The

new money data GD is stored as data at the access address ZA in the second storage location

23 by the first access approval means 37 during a write access. This access concludes the

entry of money data GD to be entered and corresponding to one hundred Euro and the access

status ZS is communicated to the second data processing means 31 by the second memory

15   access means 33 via the status reception buffer 35 and is subsequently communicated to the

second communication device 3 in the form of second reception data ED2, upon which the

user of the data carrier 1 is informed about the successful transaction and the communication

is terminated.

In analogy to the entry of money data GD to be entered, as described in the

20   preceding paragraph, money data GD to be deducted are deducted, for example at a cash desk

equipped to provide contact-bound communication with the data carrier 1, in the course of

which communication merely the money data GD to be deducted and corresponding to a

value of an amount to be paid should be subtracted from the old money data GD and the new

money data GD thus obtained should be stored.

25   The operation of the smart card, i.e. of the data carrier 1 in accordance with the

invention, will now be explained hereinafter with reference to a second example of use of the

data carrier 1 in the embodiment of the invention shown in Figure 1. In this second example

of use it is assumed that the data carrier 1 is made available by a second system operator,

namely a public transport company as an electronic ticket.

30   At a booking terminal transportation data BD corresponding to transportation

units are entered on payment of transportation charges during access to the first storage

location 22 of the data carrier 1. Transportation units are entered during a contactless

communication between the booking terminal, which is equipped to provide contactless

communication with the first communication device 2, and the contactless first interface 10

of the data carrier 1. Transportation units are debited during a contactless communication between an entrance gate terminal to transport means of the transport company, the entrance gate terminal also be equipped to provide contactless communication with the first communication device 2. In the second example of use it is assumed that a user wishes to add

5   five (5) transportation units to the electronic ticket, for which purpose transportation data BD to be added and corresponding to the five (5) transportation units must be stored in the memory means 17.

In order to add transportation units the data carrier 1 is brought within the communication range of the booking terminal. In accordance with the first communication

10   protocol a selection of the data carrier 1 is effected upon the start of the first operating system. Subsequently, during a communication the transportation data BD is entered into the first storage location 22 in a selected data carrier 1.

In the course of a communication between the first interface 10 and the first communication device 2 the first transmission data SD1 corresponding to the five (5)

15   transportation units to be added is communicated to the first signal conversion means 15. The first signal conversion means 15 generates first reception information EI1 from the first transmission data SD1, the contents of this first reception information in the second example of use relating to the addition of the transportation data BD to be added and corresponding to the five (5) transportation units to the data of the first storage location 22 of the memory

20   means 17. Subsequently, the first reception information EI1 is decrypted by the first data processing means 19 in accordance with the first communication protocol.

On the basis of an access address ZA included in the content of the first reception information EI1 the first data processing means 19, which forms access approval means together with the access enabling stage 21, now determines whether there is an access

25   authorization ZE for access to the first storage location 22 at the access address ZA.

When there is an access authorization ZE and when the subsequent authentication is successful the first memory access means 18 can access the transportation data BD stored in the sectors of the first storage location 22.

When there is an access authorization ZE the first data processing means 19

30   subsequently access the old transportation data BD stored at the access address ZA in the first storage location 22 so as to read the old transportation data BD. In the second example of use said old transportation data BD represent three (3) transportation units. The first data processing means 19 subsequently adds the transportation data BD to be entered and corresponding to the five (5) transportation units to the old transportation data BD. This

results in new transportation data BD which corresponds to eight (8) transportation units and which is stored as transportation data at the access address ZA in the first storage location 23 during the write access. This access terminates the entry of transportation data BD to be added and representing five (5) transportation units. The termination of the entry is

5   communicated to the contactless first communication device 2 of the booking terminal in the form of first receiving data ED1, upon which the user of the data carrier 1 is informed about the successful transaction and the communication is terminated.

The deduction of transportation data BD to be deducted is effected in analogy to the entry of transportation data BD to be added as described hereinbefore, the first data

10   processing means 19 merely subtracting the transportation data BD to be deducted from the old transportation data BD in the course of a communication and storing the new transportation data BD thus obtained.

The operation of the smart card, i.e. of the data carrier 1 in accordance with the invention, will now be explained hereinafter with reference to a third example of use of the

15   data carrier 1 in the embodiment of the invention shown in Figure 1. In this third example of use it is now assumed that the banking company and the transport company cooperate and that it should be possible to enter transportation units into the first storage location 22 at a bank terminal, i.e. booking terminal.

For this purpose, the data carrier 1 has additional memory access means 38

20   provided in accordance with the invention.

The additional memory access means 38 are adapted to cooperate with the second memory access means 33 and to gain access to the first storage location 22 and to verify an access authorization in such a manner that after a positive result of the verification of the access authorization the second memory access means 33 can also access the first

25   storage location 22 via the additional memory access means 38 and via the first memory access means 18.

This yields the advantage that during a contact-bound communication with a bank terminal via the second interface 25 the second operating system 30 can access the first storage location 22 via the first operating system 16 after the verification of an access

30   authorization and after having received a positive verification result. This guarantees a high level of protection against unauthorized access to the storage locations of the systems during cooperation of the two system operators.

A further advantage is that the provision of a verification of an access authorization enables a flexible structure as well as a flexible management of this access

authorization to be achieved. For example, in the case of an incorrect use of the data carrier 1 any further use of the data carrier as an electronic ticket can be inhibited in a very simple manner, in conjunction with the inventive measures, during a contactless communication with an entrance gate terminal of the transport company, although the data carrier 1 can

5   subsequently be used as an electronic wallet without any restriction. Moreover, the advantage is obtained that software routines already used in the first operating system can be utilized, as a result of which the characteristic features of the invention can be realized in a particularly simple manner.

The additional memory access means 38 are included in the first memory

10   access means 18 and have a second access approval means 39 which on account of an applicable access address ZA together with the access enabling stage 21 forms access enabling means adapted to determine an access authorization ZE for the memory means 17.

This yields the advantage that it remains possible to prevent a direct access to the first storage location 22 by the second operating system 30 with the aid of the access

15   enabling means. However, as a result of the presence of an access authorization for an access by additional memory access means 38 included in the first operating system 16, the second operating system 30 can access the first storage location 22 via the additional memory access means 38. Moreover, the prevention of a direct access to the first storage location 22 by the second operating system 30 ensures that the access to the transportation units proceeds in a

20   wholly consistent manner because access is possible only with a part of the first operating system 16, i.e. the additional memory access means 38. This precludes an incorrect access, such as for example an incorrect writing of transportation data into the first storage location 22 by the second operating system 30 of the banking company.

The additional memory access means 38 further include additional code

25   verification means for the verification of an access code. The access verification means 40 is shown symbolically as an AND gate, which can supply a first verification result B1 to a verification result logic means 41, which is also shown symbolically as an AND gate. The first verification result B1 is also made available to the second operating system 30 via the status reception buffer 35. The access code verification means 40 can receive a first access

30   code ZC1 from the second memory access means 33 via the access request buffer 34 and can also receive a second access code ZC2, which can be calculated by means of the first key and the second key, which are stored in the first storage location 22. A positive result of the access authorization verification requires correspondence between the first access code ZC1 and the second access code ZC2.

This yields the advantage that there is maximal flexibility as regards the source of the access code ZC1 that can be applied. Thus, the applicable access code ZC1 can be communicated advantageously during a communication between the data carrier 1 and a contact-bound communication device 3, which is particularly useful when an applicable

5   access code ZC1 should be available for each user. It may also be advantageous to store the applicable access code ZC1 in the second storage location 23 if the user is not required to re-enter the applicable access code ZC1 via the bank terminal upon each entry of transportation units. Furthermore, in the case that extreme requirements are imposed on the secrecy of the applicable access code ZC1, it may also be advantageous to calculate the applicable access

10   code ZC1 from data transmitted during a communication or from data stored in the memory means 17 by means of the second data processing means 31.

The additional memory access means 38 further includes an access code calculation means 41 for the calculation of the calculable second access code ZC2, which access code calculation means is adapted to execute a triple DES encryption process in

15   accordance with the ISO/IEC 10116 standard. In the case that there is an access authorization ZE for an access address ZA the second access approval means 39 access a sector of the first storage location 22 whose address is defined by the access address ZA to read the first key and the second key. The first key and the second key are applied to the access code calculation means 42 with the aid of the second access approval means 39, thus enabling the

20   calculation of the second access code ZC2, which is carried out by the access code calculation means 42. It is to be noted that the triple DES encryption process requires the first key and the second key for the calculation of the second access code ZC2.

This yields the advantage that the keys used as the basis for the authentication in accordance with the first communication protocol during the access to the sectors of the

25   first storage location can subsequently be kept secret and the banking company should merely know the access code ZC1 that can be calculated from the keys.

Moreover, this yields the advantage that the calculation of the second access code ZC2 is speeded up significantly, because the access code calculation means 42 suitably takes the form of a crypto-coprocessor.

30   A further advantage is obtained in that the use of the triple DES encryption process precludes a reversal of the calculation in order to determine the keys.

In addition to the access code verification means 40 the additional memory access means 38 include access condition verification means 43 for the verification of an access condition. The access condition verification means 43 is shown symbolically as an

AND gate, which can supply a second verification result B2 to the verification result logic means 41. The access condition verification means 43 can receive a first access condition ZB1 from the second memory access means 33 via the access request buffer 34 and can also receive a second access condition ZB2, which can be derived from the data in the first

5   storage location 22 as the sector access condition. If there is an access authorization ZE for an access address ZA the second access approval means 39 access data of a sector of the first storage location 22 whose address is defined by means of the access address ZA, said data representing the sector access authorization. The sector access authorization is read by the second access approval means 39 and is applied to the access condition verification means 43

10   as the second access condition ZB2.

This yields the advantage that for the protection against unauthorized access to the first storage location 22, in addition to the verification of the access code ZC1, a verification of the access condition ZB1 is provided during the verification of access authorizations. Thus, even in the case of correspondence of an applicable access code to a

15   calculable access code, an additional verification may be carried out before finally a positive result of the verification of the access authorization is obtained in the case that these access conditions are also in agreement. This measure enables a hierarchical allocation of the access authorization. For example, during communication of the data carrier 1 with the contactless communication device 2 of an entrance gate terminal of the transport company a problem

20   with the debiting of transportation units may arise which cannot be solved on the spot. This problem may be, for example, a serious deficit on the balance of transportation units stored on the data carrier. During the communication the entrance gate terminal can now alter an access condition for transportation data BD corresponding to the transportation units in such a manner that an addition of transportation units at a bank terminal is no longer possible even

25   when a valid access code is entered. During the communication with the bank terminal it is then possible to display a message for the user, requesting him to go to a booking terminal to solve the current problem. When a problem has occurred during a correct use of the data carrier 1 a re-allocation of the access code ZC1 is therefore not compulsive with the hierarchical allocation of the access authorization. The problem that has arisen can be

30   explained to the user at the booking terminal and, if necessary, the access condition for the transportation data BD corresponding to the transportation units can be altered so as to enable transportation data BD corresponding to transportation units to be entered again at a bank terminal.

A prerequisite for a positive result of the verification of the access authorization is agreement between the first access code ZC1 and the second access code ZC2, as represented by the first verification result B1, as well as agreement between the first access condition ZB1 and the second access condition ZB2, as represented by the second

5   verification result B2. The result of the verification of the access authorization is generated with the aid of the verification result logic means 41, which is shown symbolically as an AND gate, and is transferred as a third verification result B3 to the second access approval means 39 as well as to the status reception buffer 35.

In the second example of use it is assumed that the user of the data carrier 1

10   withdraws one hundred Euro from his account at a bank terminal and at the same time loads transportation units to the amount of one hundred Euro into the first storage location 22 of the data carrier 1 at the bank terminal, in which storage location 22 old transportation data BD corresponding to transportation units of the transport company is stored. For this purpose, the user inserts the smart card into a slot of the bant terminal, upon which a contact-bound

15   communication via the contact pair 9 begins. The user subsequently identifies himself as the legitimate user for the second operating system of the banking company. With the aid of an entry console he expresses the wish to load transportation units into the memory means 17 of the data carrier 1 and to pay these transportation units directly through his account with the banking company. He is prompted to enter the amount to be spent on transportation units into

20   the bank terminal. Subsequently, he is prompted the enter the first access code ZC1, with which he identifies himself as a legitimate user for the second operating system of the transport company.

In the third example of use, during a subsequently started communication between the second interface 25 and the second transmitting/receiving means 7 of the second

25   communication device 3, it is now also possible that second reception information EI2 occurs, whose content relates to the entry of transportation data BD corresponding to the transportation units to be added into the first storage location 22. The second reception information EI2 is received by the second operating system 30 and is applied from the second data processing means 31 to the interface means 32, where the access parameters ZP are

30   applied to the additional memory access means 38 via the second memory access means 33. Moreover, via the access request buffer 34, the first access code ZC1 is applied to the access code verification means 40 and the first access condition ZB1 is applied to the access condition verification means 43.

Hereinafter, the access to the first storage location 22 of the memory means 17 of the data carrier 1 by means of a method in accordance with the invention is described, which is represented by the flow chart 44 shown in Figure 2.

The execution of the method 44 in accordance with the invention starts in a block 45, when the access parameters ZP are applied to the access request buffer 34.

In a following block 46 the access enabling means formed by the second access approval means 39 and the access enabling stage 21 first determine on the basis of the access address ZA whether there is an access authorization ZE for an access address ZA of the first storage location 22.

In the absence of an access authorization ZE the second operating system 30 is informed about the access status ZS, that access is not allowed, via the status reception buffer 35 in a block 47. Subsequently, the second operating system 30 communicates the access status ZS to the second communication device 3 and the memory access means 38 discontinues the access to the first storage location 22, upon which the method 44 in accordance with the invention is terminated in the block 48.

If the case that there is an access authorization ZE the access code calculation means 42 subsequently calculates the calculable second access code ZC2 in a block 49.

Subsequently, in a block 50, the calculable second access code ZC2 is compared with the applicable first access code ZC1 with the aid of the access code verification means 40. On the basis of the first verification result B1 thus obtained it is decided whether the access may be continued or is to be discontinued.

In the case that there is no agreement between the first access code ZC1 and the second access code ZC2 the method 44 proceeds to the block 47 and is terminated in the block 48.

In the case that there is agreement between the first access code ZC1 and the second access code ZC2 the method 44 proceeds to a block 51, in which the first access condition ZB1 and the second access condition ZB2 are compared and a second verification result B2 is obtained. On the basis of the verification result B2 thus obtained it is decided whether the access is continued or whether the access is to be discontinued.

In the case that there is no agreement between the first access condition ZB1 and the second access condition ZB2 the method 44 proceeds to the block 47 and is terminated in the block 48. In the case that there is agreement between the first access condition ZB1 and the second access condition ZB2 the method 44 proceeds to a block 52, in

which the storage location 22 is accessed and access is subsequently terminated in the block 48.

During said access to the first storage location 22 the old transportation data BD is read first of all with the aid of the second access approval means 39 and the old

5   transportation data BD is transferred to the second data processing means 31 via the access data buffer BD, in which data processing means the old transportation data BD is added to the transportation data BD to be entered. The new transportation data BD thus obtained is transferred to the second access approval means 39 via the access data buffer 36 and is stored as data by the second access approval means 39 at the access address ZA in the first storage

10   location 22 during a write access. Thus, the transportation units to the amount of one hundred schilling are stored in the first storage location 22 of the transport company as transportation data BD to be entered.

Thus, in the third example of use the second communication device 3 of the second system operator merely needs to know a first access code ZC1, which can be

15   calculated from two keys of a sector of the first storage location 22 by means of a triple DES process and which is identical to the second access code ZC2. In the present case the first access code ZC1 has been made available to the second communication device 3 via the bank terminal during entry of the first access code ZC1. Consequently, it is achieved that by means of the additional memory access means 38 in accordance with the invention access to the first

20   storage location 22 is possible during a communication via the contact-bound second interface 25 of the data carrier 1, although only the first system operator knows the keys of the sectors of the first storage location 22. This guarantees the protection, required by the first system operator, against unauthorized access to data stored in the first storage location 22 during a cooperation between the two system operators. In addition to this protection this has

25   the advantage for the user of the data carrier 1 that he can enter transportation units directly at a bank terminal and thus saves additional time.

It is to be noted that during access to the memory means 17 the means 19, 37, 39, which together with the access enabling stage 21 form access enabling means, can access a common software routine which forms part of the first operating system 16.

30   It is to be noted that the access enabling means and the additional memory access means 38 provided in accordance with the invention form parts of a master operating system which ranks higher than one or more other operating systems and that access to the memory means 17 is possible only with the aid of these two parts.

It is to be noted that the data carrier 1 in accordance with the invention may form part of a key or a key fob. Moreover, the data carrier 1 in accordance with the invention may form part of a piece of jewelry such as for example a watch or a ring. Moreover, it is to be mentioned that a data carrier 1 in accordance with the invention may be part of a writing

5   instrument such as for example a ballpoint pen.

It is to be noted that a known data carrier 1 may include an interface switching means. The interface switching means serves to switch between the first interface 10 for contactless communication with a contactless communication device 2 and the second interface 25 for contact-bound communication with a contact-bound communication device 3

10   during the operation of the second operating system 30. The interface switching means enables the second operating system 30 to access the first storage location 22 via the first operating system 22 both during communication via the first interface 10 and during communication via the second interface 25, as a result of which for example the banking company has the possibility of both contactless communication and contact-bound

15   communication via the bank terminal. In this respect it is to be noted as well that the interface switching means may also enable contactless communication as well as contact-bound communication during operation of the first operating system.

It is to be noted that an entrance gate terminal may be formed by a turnstile or an entrance barrier equipped with a contactless communication device 2. In the case of an

20   appropriate communication range of the contactless communication device 2 a part of the entrance gate terminal may alternatively be formed by a carpet, or a part of a floor, or a part of a wall covering or a ceiling covering, in which part the primary coil 5 of the contactless communication device 2 has been integrated. An entrance gate terminal is to be understood to mean also a mobile ticket cancellation station having a contactless communication device and

25   carried, for example, by a conductor.

CLAIMS:

1.   A data carrier (1) for the storage of data,

which data carrier (1) has a first interface (10) for communication with a first communication device (2) and

which data carrier (1) has a second interface (25) for communication with a second

5   communication device (3) and

which data carrier (1) includes an electrical circuit arrangement (12),

which circuit arrangement (12) includes circuit parts (13, 14, 15) of the first interface (10) and circuit parts (27, 28, 29) of the second interface (25) and

which circuit arrangement (12) has memory means (17) for the storage of data, which

10   memory means (17) has a first storage location (22) and a second storage location (23), and

which circuit arrangement (12) has a first memory access means (18), arranged between the first interface (10) and the memory means (17), for accessing the memory means (17) and

which circuit arrangement (12) has a second memory access means (33), arranged between the second interface (25) and the memory means (17), for accessing the memory means (17)

15   and

which circuit arrangement (12) has access enabling means (21, 37, 39, 19) which enable the first storage location (22) to be accessed only by the first memory access means (18), characterized

in that the data carrier (1) has additional memory access means (38) adapted to cooperate

20   with the second memory access means (33) and adapted to access the first storage location (22) and designed to verify an access authorization for the access to the first storage location (22), and

in that after a positive result of the verification of the access authorization the second memory access means (33) can, in addition, access the first storage location (22) via the

25   additional memory access means (38) and via the first memory access means (18).

2.   A data carrier (1) as claimed in Claim 1, characterized in that the additional memory access means (38) are included in the first memory access means (18).

3.   A data carrier (1) as claimed in Claim 1, characterized

in that the additional memory access means (38) include access code verification means (40)

for the verification of an access code (ZC1), and

5   in that a first access code (ZC1) from the second memory access means (33) as well as a

second access code (ZC2) can be applied to the access code verification means (40), which

second access code can be calculated from data stored in the first storage location (22), and

in that agreement of the first access code (ZC1) and the second access code (ZC2) is

prerequisite for the positive result of the verification of the access authorization.

10

4.   A data carrier (1) as claimed in Claim 3, characterized

in that an access code calculation means (42) has been provided for the calculation of the

calculable second access code (ZC2), and

in that the access code calculation means (42) is adapted to execute a triple DES encryption

15   process.

5.   A data carrier (1) as claimed in Claim 3, characterized

in that the additional memory access means (38) have, in addition to the access code

verification means (40), access condition verification means (43) for the verification of an

20   access condition (ZB1), and

in that a first access condition (ZB1) from the second memory access means (33) as well as a

second access condition (ZB2) can be applied to the access condition verification means (43),

which second access condition can be determined from data stored in the first storage

location (22), and

25   in that agreement of the first access code (ZC1) and the second access code (ZC2) as well as

agreement of the first access condition (ZB1) and the second access condition (ZB2) are

prerequisite for the positive result of the verification of the access authorization.

6.   A data carrier (1) as claimed in Claim 1, characterized

30   in that the electrical circuit arrangement (12) of the data carrier (1) takes the form of an

integrated circuit.

7.   An electrical circuit arrangement (12) for a data carrier (1) for the storage of

data,

which circuit arrangement (12) includes circuit parts (13, 14, 15) of a first interface for

communication with a first communication device (2) and

which circuit arrangement (12) includes circuit parts (27, 28, 29) of a second interface (25)

for communication with a second communication device (3) and

5   which circuit arrangement (12) has memory means (17) for the storage of data, which

memory means (17) has a first storage location (22) and a second storage location (23), and

which circuit arrangement (12) has a first memory access means (18), arranged between the

circuit parts (13, 14, 15) of the first interface (10) and the memory means (17), for accessing

the memory means (17) and

10   which circuit arrangement (12) has a second memory access means (33), arranged between

the circuit parts (27, 28, 29) of the second interface (25) and the memory means (17), for

accessing the memory means (17) and

which circuit arrangement (12) has access enabling means (21, 37, 39, 19) which enable the

first storage location (22) to be accessed only by the first memory access means (18),

15   characterized

in that the circuit arrangement (12) has additional memory access means (38) adapted to

cooperate with the second memory access means (33) and adapted to access the first storage

location (22) and designed to verify an access authorization for the access to the first storage

location (22), and

20   in that after a positive result of the verification of the access authorization the second

memory access means (33) can, in addition, access the first storage location (22) via the

additional memory access means (38) and via the first memory access means (18).

8.   A circuit arrangement (12) as claimed in Claim 7, characterized

25   in that the additional memory access means (38) are included in the first memory access

means (18).

9.   A circuit arrangement (12) as claimed in Claim 7, characterized

in that the additional memory access means (38) include access code verification means (40)

30   for the verification of an access code (ZC1), and

in that a first access code (ZC1) from the second memory access means (33) as well as a

second access code (ZC2) can be applied to the access code verification means (40), which

second access code can be calculated from data stored in the first storage location (22), and

in that agreement of the first access code (ZC1) and the second access code (ZC2) is prerequisite for the positive result of the verification of the access authorization.

10.   A circuit arrangement (12) as claimed in Claim 9, characterized
in that an access code calculation means (42) has been provided for the calculation of the calculable second access code (ZC2), and
in that the access code calculation means (42) is adapted to execute a triple DES encryption process.

11.   A circuit arrangement (12) as claimed in Claim 9, characterized
in that the additional memory access means (38) have, in addition to the access code verification means (40), access condition verification means (43) for the verification of an access condition (ZB1), and
in that a first access condition (ZB1) from the second memory access means (33) as well as a second access condition (ZB2) can be applied to the access condition verification means (43), which second access condition can be determined from data stored in the first storage location (22), and
in that agreement of the first access code (ZC1) and the second access code (ZC2) as well as agreement of the first access condition (ZB1) and the second access condition (ZB2) are prerequisite for the positive result of the verification of the access authorization.

12.   A circuit arrangement (12) as claimed in Claim 7, characterized
in that the electrical circuit arrangement (12) takes the form of an integrated circuit.

13.   A method (44) of accessing memory means (17) of a data carrier (1) having a first storage location (22) and a second storage location (23), the method (44) comprising the steps defined hereinafter, namely
storing data in at least the first storage location (22) of the memory means (17),
enabling the first storage location (22) to be accessed only by the first memory access means (18),
characterized
in that access authorizations for access to the first storage location (22) are applied to additional memory access means (38), and

in that the applied access authorizations are verified with the aid of the additional memory access means (38), and

in that after verification of the access authorizations and in the case of a positive result of the verification the first storage location (22) is accessed additionally by a second memory access

5   means (33) via the additional memory access means (38) and via the first memory access means (18).

14.   A method (44) as claimed in Claim 13, characterized

in that during the verification of the access authorizations a first access code (ZC1) is

10   compared with a second access code (ZC2) by means of access code verification means (40), and

in that the first access code (ZC1) is applied from the second memory access means (33), and the second access code (ZC2) is calculated from data stored in the first storage location (22), and

15   in that agreement of the first access code (ZC1) and the second access code (ZC2) is prerequisite for the positive result of the verification.

15.   A method (44) as claimed in Claim 14, characterized

in that during the verification of the access authorizations, in addition to the comparison of

20   the first access code (ZC1) and the second access code (ZC2) with the aid of the access code verification means (40), a first access condition (ZB1) is compared with a second access condition (ZB2) with the aid of access condition verification means (43), and

in that the first access condition (ZB1) is applied from the second memory access means (33) to the access condition verification means (43) and the second access condition (ZB1) is

25   determined from data stored in the first storage location (22), and

in that agreement of the first access code (ZC1) and the second access code (ZC2) as well as agreement of the first access condition (ZB1) and the second access condition (ZB2) are prerequisite for the positive result of the verification.

ABSTRACT:

A data carrier (1) intended for the storage of data in memory means (17) has a first memory access means (18) for accessing a first storage location (22) and has a second memory access means (33) for accessing a second storage location (23), the first storage location (22) being only accessible by the first memory access means (18) with the aid of access enabling means (21, 19, 37, 39), and further has an additional memory access means (38), so as to enable an access authorization for the access to the first storage location (22) and so as to enable access to the first storage location (22) during an access by the second memory access means (33).
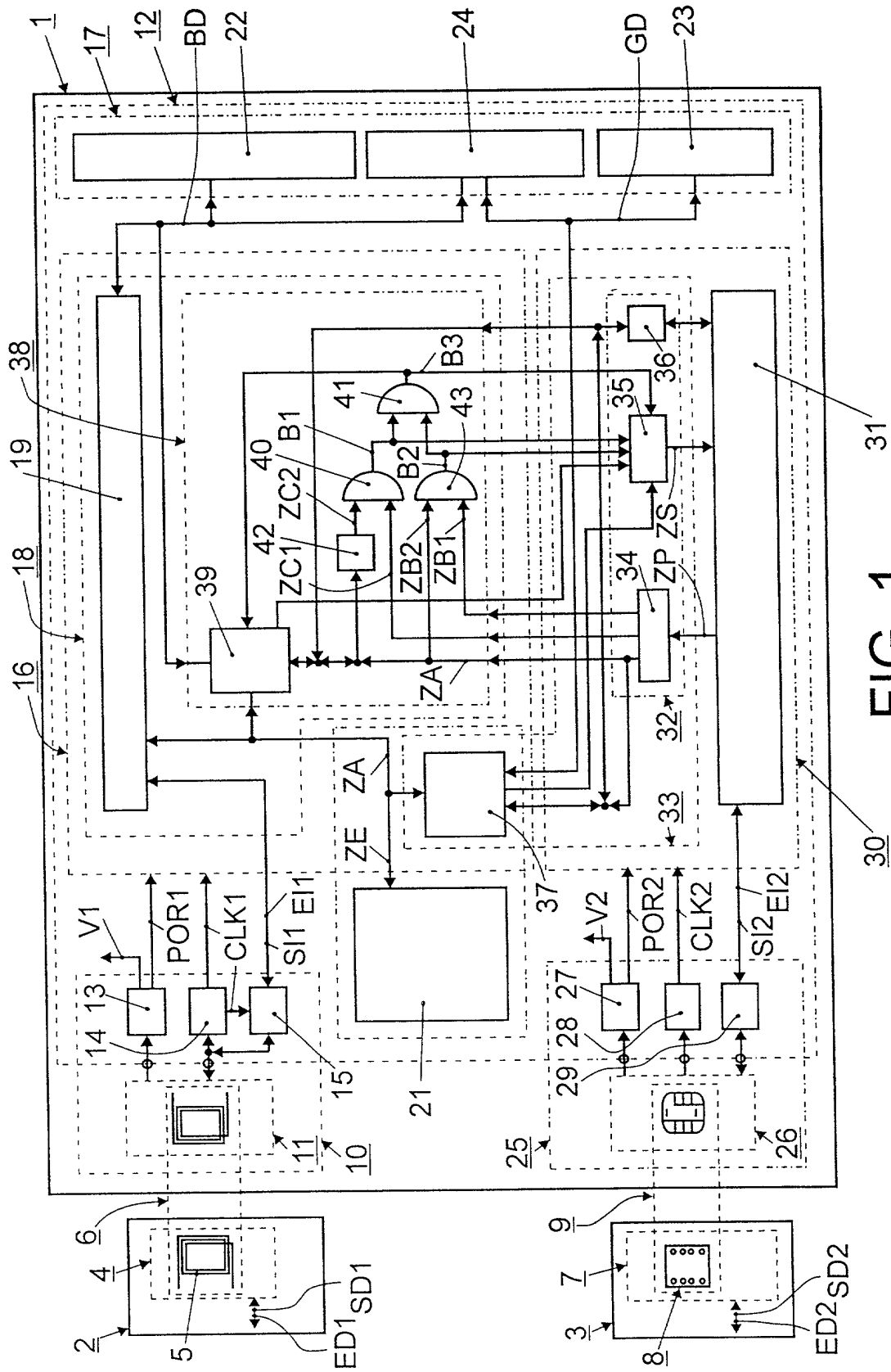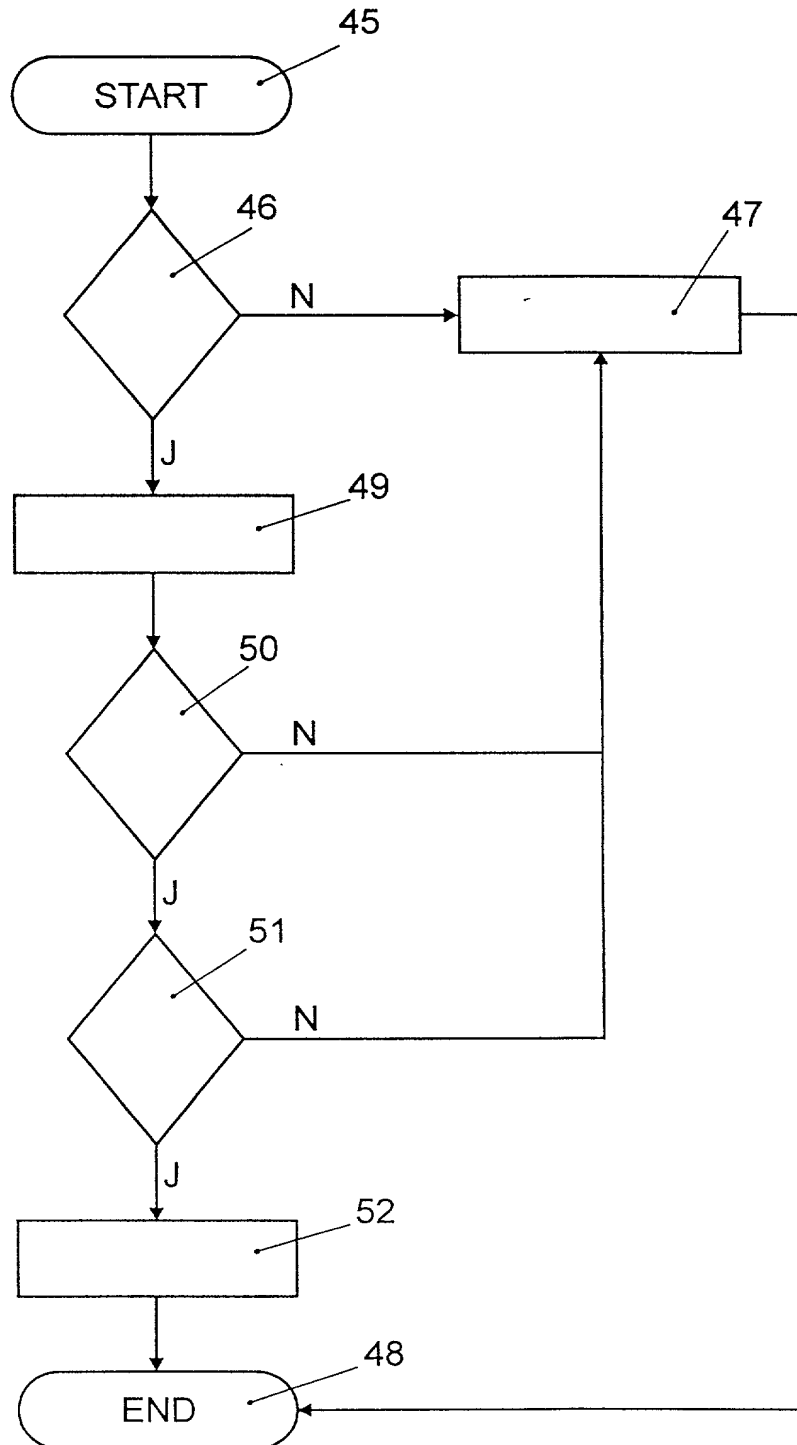
Fig. 1

FIG. 1

44

45 START

46

47

J

49

50 N

51 N

J

52

48 END

FIG. 2

DECLARATION and POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

"Data carrier for the storage of data and circuit arrangement for such a data carrier"

the specification of which (check one)

☐ is attached hereto.

☐ was filed on _____ as Application Serial No. _____ and was amended on

_____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.

I acknowledge the duty to disclose information which is material to patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APP. NUMBER	DATE OF FILING (DATE, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119
Europe	**99890248.0**	**22 July 1999**	**YES**

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1,56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PRIOR UNITED STATES APPLICATION(S)

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Algy Tamoshunas, Reg. No. 27,677
Jack E. Haken, Reg. No. 26,902

SEND CORRESPONDENCE TO: Corporate Patent Counsel; U.S. Philips Corporation; 580 white Plains Road; Tarrytown, NY 10591	DIRECT TELEPHONE CALLS TO: (name and telephone No.) (914) 332-0222

Dated:	Inventor's Signature:		
Full Name of in Inventor	Last Name **MÜHLBERGER**	First Name **Andreas**	Middle Name
Residence & Citizenship	City **Graz**	State of Foreign Country **Austria**	Country of Citizenship **Austria**

Post Office Address	Street **Falkenhofgasse 31**	City **A-8020 Graz**	State of Country **Austria**	Zip Code

Dated:	Inventor's Signature:		
Full Name of in Inventor	Last Name **POSCH**	First Name **Stefan**	Middle Name
Residence & Citizenship	City **Gratkorn**	State of Foreign Country **Austria**	Country of Citizenship **Austria**

Post Office Address	Street **Statteggerstraße 52/5**	City **A-8101 Gratkorn**	State of Country **Austria**	Zip Code